Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program	)	EA Docket No. 21-233
	)	

REPLY COMMENTS OF CHARTER COMMUNICATIONS, INC.

Charter Communications, Inc. ("Charter") respectfully submits these reply comments on the Federal Communications Commission's (the "Commission") Notice of Inquiry ("NOI") in the above captioned matter.[1]

INTRODUCTION AND SUMMARY

The growing proliferation of cybersecurity incidents in recent years underscores the need for a whole-of-government effort to address and deter cyber threats. These threats often exploit internet of things ("IoT") devices like network-connected baby monitors or garage door openers that lack strong passwords and are therefore easily compromised to become a source for harmful and malicious traffic. Devices that can connect to home networks without authentication are a significant source of cyber threats. Charter therefore supports the Commission's proposal to use its equipment authorization program to help improve cybersecurity by minimizing the likelihood

[1] *In re Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Notice of Proposed Rulemaking and Notice of Inquiry, ET Docket No. 21-232, FCC 21-73 (rel. June 17, 2021) ("*NPRM and NOI*").

that devices it approves will threaten the integrity of communications networks.[2] Because equipment manufacturers who make and sell these connected devices are in the best position to address common security vulnerabilities in these devices, the Commission can and should use its equipment authorization authority to require that these devices come equipped with reasonable cybersecurity safeguards.

In particular, Charter encourages the Commission to authorize only consumer devices that can deter these threats by requiring users to set strong on-device administrative passwords and requiring that such devices affirmatively seek and obtain appropriate authorization before the device can connect to that broadband network. Requiring device manufacturers to build in affirmative authentication capabilities would be a cost-efficient safeguard against cybersecurity attacks. These basic requirements would significantly enhance the security of devices without the need for the Commission to prescribe any detailed cybersecurity standards.

This approach would also be an effective way for the Commission to support and complement other governmental efforts to enhance cybersecurity, including by the Federal Trade Commission, Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA"), and the National Institute for Standards and Technology ("NIST").[3] All of these agencies recommend that consumers secure their devices against unauthorized users, including by changing default passwords and establishing strong passwords. Device manufacturers are in the best position to provide these basic safeguards, and the equipment

---

[2] *NPRM and NOI* ¶ 102.

[3] Federal Trade Commission, *How To Secure Your Home Wi-Fi Network* (May 2021), https://www.consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network#limit; Cybersecurity & Infrastructure Security Agency, *Security Tip (ST05-003) Securing Wireless Networks* (last revised May 8, 2020), https://us-cert.cisa.gov/ncas/tips/ST05-003 ("CISA Guidance"); Michael Fagan et al., National Institute of Standards and Technology, NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* (May 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf.

authorization program is therefore the most appropriate vehicle for ensuring they are put in place. The combination of enhanced equipment authorization requirements and active engagement by device users will better protect Americans and U.S. networks from the growing harm of cyber threats.

I. MALICIOUS AND UNLAWFUL TRAFFIC REMAINS A CONSTANT THREAT TO DOMESTIC BROADBAND NETWORKS.

Broadband networks in the United States face a constant and growing threat from malicious network traffic. Ninety percent of all IoT cyberattacks that occurred in 2018 were carried out through in-home networking devices.[4] The risk of cyber threats to U.S. networks will only increase as more and more consumer devices are being connected to residential and business networks. Charter estimates that more than 450 million devices are connected to its network. Many of these devices are potentially vectors through which hackers can carry out cyberattacks directly, or indirectly by infecting routers and other interface devices that can in turn be used to engage in cyberattacks.

"[M]alicious cyber campaigns … threaten the public sector, the private sector, and ultimately the American people's security and privacy."[5] Cyberattacks conducted through unsecured consumer devices also raise national security threats, including potentially threatening critical physical infrastructure, such as water and power, and financial institutions.[6] For example,

---

[4] Symantec, *ISTR - Internet Security Threat Report* at 20 (Feb. 2019), https://docs.broadcom.com/doc/istr-24-2019-en ("Symantec Report").

[5] Executive Order 14028, *Improving the Nation's Cybersecurity*, 86 Fed. Reg. 26633 § 1 (May 12, 2021) ("EO"); *see also NPRM and NOI* ¶ 65.

[6] *See, e.g.*, Suzanne E. Spaulding, *Keeping Our Critical Infrastructure Cyber-Secure*, Department of Homeland Security BLOG (Oct. 20, 2014, 10:21 AM), https://www.dhs.gov/blog/2014/10/20/keeping-our-critical-infrastructure-cyber-secure (noting that, "[w]hile cyber-dependent networks and devices offer greater convenience and efficiency, they also come with potential risks and threats to our security," and particularly our "critical infrastructure" as it is becoming "more dependent on the internet"); Press Release, Department of Homeland Security, *Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity* (Dec. 29, 2016), https://www.

in April 2018, CISA issued an alert warning that cyber-actors supported by the Russian government had carried out a multi-year campaign to exploit security vulnerabilities in network devices to enable espionage and intellectual property theft.[7] Because of the insufficient security found in many consumer devices that connect to broadband networks, hostile actors can exploit these devices to launch crippling DDoS attacks on domestic network infrastructure or to unlawfully use broadband networks to engage in a variety of other harmful and criminal schemes. In light of these persistent threats, it is essential to "ensure . . . products are built and operate securely."[8] The proliferation of new devices will introduce more ambiguity to systems already faced with substantial cybersecurity risk.

Third-party and consumer IoT devices present the most salient risks in this regard, as cable and other network service providers have consistently and proactively enhanced the identification and authentication features of in-home devices like modems and routers for decades. For instance, "nearly 20 years ago, CableLabs adopted PKI-based digital certificates to support strong device identity and authentication for devices connecting directly to the cable network (e.g., cable modems, Internet gateways, set-top boxes)."[9] PKI utilizes digital certificates installed during manufacturing to verify the identity of devices connecting to the network to facilitate secure electronic communication and data exchange. Since the initial implementation, CableLabs has

---

dhs.gov/news/2016/12/29/joint-dhs-odni-fbi-statement-russian-malicious-cyber-activity (describing cyber-enabled operations directed at the U.S. Government and its citizens as part of a decade-long campaign, which included "spearphishing, campaigns targeting government organizations, critical infrastructure, think tanks, universities, political organizations, and corporations; theft of information from these organizations; and the . . . public release of some of this stolen information").

[7] Cybersecurity and Infrastructure Security Agency, *Alert (TA18-106A): Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices* (last revised Apr. 20, 2018), https://www.us-cert.gov/ncas/alerts/TA18-106A.

[8] EO § 1.

[9] *See* Mark Walker, *Driving Increased Security in All IoT Devices*, CableLabs (Sept. 18, 2019).

continued to advance its PKI implementation to address new and emerging threats. CableLabs also earlier this month released a set of Gateway Device Security Best Practices to standardize robust network security practices across cable modems, integrated access points, and home routers.[10] Those best practices emphasize authentication and identity management as key tools to enhancing broadband network security.

Downstream device vulnerability was at the heart of some of the biggest network attacks in recent years. The Mirai Botnet DDoS attack, the largest-ever to date, targeted personal connected devices that were easily compromised because they were secured only by weak default passwords.[11] Cyberattacks by copycats and similar botnets have proven to be a growing cause for concern. Ransomware attacks are also accelerating at an alarming rate. The daily average number of ransomware attacks increased by 50 percent worldwide during the first half of 2020, with the U.S. experiencing the greatest increase at 98.1 percent.[12]

II. THE COMMISSION SHOULD ADOPT AFFIRMATIVE AUTHENTICATION REQUIREMENTS.

In order to minimize the risks to broadband networks from unsecured consumer devices, the Commission should leverage its equipment authorization program by requiring device manufacturers to include safeguards against major cybersecurity vulnerabilities. First, the device should prompt the end-user to set a new on-device administrative password as part of the set-up process or upon first use. This requirement would make each device less susceptible to attackers

---

[10] CableLabs, CL-GL-GDS-BCP-V01-211007, *Gateway Device Security Best Common Practices* (Oct. 7, 2021), https://www.cablelabs.com/specifications/CL-GL-GDS-BCP.

[11] *See* David Strom, *IoT security: 8 lessons learned from the Mirai botnet*, enterprise.nxt (Feb. 1, 2017).

[12] Chuck Brooks, *Cybersecurity Threats: The Daunting Challenge of Securing the Internet of Things*, Forbes (Feb. 7, 2021), https://www.forbes.com/sites/chuckbrooks/2021/02/07/cybersecurity-threats-the-daunting-challenge-of-securing-the-internet-of-things/?sh=1bbf9015d500; *Global Surges in Ransomware Attacks*, Check Point BLOG (Oct. 6, 2020), https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks/.

who could exploit default passwords to compromise the devices. Second, a device's operating system should prevent the device from connecting to a broadband network without appropriate authorization. Requiring authentication before connection would limit the opportunity for malicious actors to exploit unsecured devices to connect to broadband networks without the device user's or the network owner's consent.

Adopting these requirements would be a simple and efficient way to address major cybersecurity vulnerabilities, without the need for the Commission to prescribe detailed cybersecurity requirements, either for service providers or equipment manufacturers. Taken together, these requirements would help ensure that all new IoT devices offer a baseline access control functionality that would make it much more difficult for unauthorized users, like Mirai copycats, to infect consumer devices and access large numbers of new attack vectors.

The bright-line rules proposed above establish a baseline applicable to consumer devices of all risk levels, which would ameliorate substantial and growing—yet easily addressed—vulnerabilities, which have been shown to present substantial risks to U.S. networks. Unsecured devices with weak authentication requirements are a primary weak point—if not *the* primary weak point—exploited by malicious actors. In recent years, most IoT data breaches were attributable to weak, default, or easily predicted passwords. And most consumers never change the default passwords on their devices.[13]

[13] Mark McFadden, Sam Wood, Robindhra Mangtani, & Grant Forsyth, *The Economics of the Security of Consumer-Grade IoT Products and Services*, Internet Society at 34 (Apr. 2019), https://www.internetsociety.org/wp-content/uploads/2019/04/The_Economics_of_Consumer_IoT_Security.pdf; Rear Adm. (ret.) David Simpson Comments on Equipment Authorization NOI at 6, ET Docket No. 21-232, EA Docket No. 21-233 (Sept. 20, 2021) ("Simpson Comments").

The Commission's equipment authorization program could be used to require a minimum level of security for specific types of high risk devices.[14] The establishment of clear identity, certification, and authorization descriptions and obligations for device deployment and integration would provide much needed confidence for enterprises wanting to deploy IoT functions across heterogeneous network environments. Through its role in equipment authorization, the Commission is well positioned to address this key vulnerability in the internet ecosystem and should undertake the measures necessary to do so.

Federal guidelines for IoT security also emphasize that consumers should take steps to prevent devices from becoming a source of cyber harms.[15] For instance, the FTC has recognized it is incumbent upon manufacturers to incorporate certain security features into the design of their devices, and encourages companies to design IoT devices in a way that results in the use of "unique" passwords by "requiring consumers to change the [default] password during set-up."[16] CISA has similarly argued that changing default passwords is a critical means of protecting

[14] Comments of Intertek at 1, ET Docket No. 21-232 (Sept. 20, 2021) ("Intertek Comments").

[15] Comments of CTIA at 34, ET Docket No. 21-232, EA Docket No. 21-233 (Sept. 20, 2021) (discussing how the FCC can help consumers "improve basic cyber hygiene and be responsible digital citizens that use secure password practices and accepted devices"); Comments of the Consumer Technology Association at 26-27, ET Docket No. 21-232, EA Docket No. 21-233 (Sept. 20, 2021) (referencing the FTC's "Careful Connections" guide, which encourages companies designing and marketing products that will be connected to the Internet of Things to require consumers to change default passwords); Simpson Comments at 5-6.

[16] FTC, *Careful Connections: Keeping the Internet of Things Secure* at 1 (Sept. 2020), https://www.ftc.gov/system/files/documents/plain-language/913a_careful_connections.pdf; *see also* FTC Staff Report, *Internet of Things: Privacy & Security in a Connected World* at 28 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf ("[C]ompanies should incorporate the use of smart defaults, such as requiring consumers to change default password – if they use default passwords at all – during the set-up process.").

wireless networks.[17] And the Commission itself has recently proposed the use of passwords for authentication purposes.[18]

Government and industry stakeholders likewise have collaborated on frameworks to secure devices that connect to broadband networks, such as the NIST Cybersecurity Framework and the NIST IoT security guidance.[19] None of these agencies has required manufacturers to incorporate the use of strong passwords in their devices, however.[20] Incorporating an affirmative network authentication requirement into the Commission's Equipment Authorization program, and requiring devices to incorporate stronger and more secure device administrative passwords, would support these federal government and industry efforts to enhance cybersecurity protections, and provide an additional layer of protection for consumers against cyber threats. Equipment manufacturers should be encouraged to take steps to follow NIST's guidance.[21]

CONCLUSION

Charter applauds the Commission's efforts to enhance the cybersecurity of broadband networks in the United States, and Charter appreciates the opportunity to recommend ways for the Commission to use its equipment authorization program to better secure domestic networks from malicious and unlawful internet traffic. Charter looks forward to working with the Commission to advance these critical goals.

---

[17] CISA Guidance.

[18] *In re Protecting Consumers from SIM Swap and Port-Out Fraud*, Notice of Proposed Rulemaking, WC Docket No. 21-341, FCC 21-102 (rel. Sept. 30, 2021).

[19] *See* Comments of 5G Americas at 5-6, ET Docket No. 21-232 (Sept. 20, 2021) (discussing the NIST Cybersecurity Framework); Simpson Comments at 6; Comments of Jennifer B. Tatel & Clete D. Johnson at 6, ET Docket No. 21-232, EA Docket No. 21-233 (Sept. 14, 2021) (encouraging the FCC to promote IoT security and private sector standards like NISTIR 8259).

[20] *See* Intertek Comments at 1.

[21] *See id.*

Dated: October 18, 2021

Respectfully submitted,

/s/ Elizabeth Andrion
Elizabeth Andrion
Senior Vice President, Regulatory Affairs

Audrey Connors
Vice President, Government Affairs

Charter Communications, Inc.
601 Massachusetts Avenue, NW
Suite 400W
Washington, DC 20001
(202) 621-1900
Elizabeth.Andrion@charter.com